CLAIMS

We claim:

1. An automated banking machine comprising:

a computer, wherein the computer includes a processor;

a transaction function device in operative connection with the computer, wherein the transaction function device includes a processor;

a first component operative in the processor of the computer, wherein the first component is operative to cause at least one first identity data to be accessed; and

a second component operative in the processor of the transaction function device, wherein the first component is operative to cause to be generated at least one first authentication hash from the at least one first identity data and at least one hashing argument, wherein the first component is operative to cause a randomly generated secret key to be generated, wherein the first component is operative to cause the randomly generated secret key to be encrypted using a public key associated with the second component, wherein the first component is operative to cause at least one message to be sent to the second component which includes the encrypted secret key and the at least

one first authentication hash, wherein the second component is operative to cause the secret key to be decrypted with a private key that corresponds to the public key, wherein the second component is operative to cause at least one second authentication hash to be compared to the first authentication hash, wherein when the at least one first authentication hash corresponds to the at least one second authentication hash, the second component is operative to enable the transaction function device to perform a transaction function in response to at least one encrypted message received from the first component.

2. The machine according to claim 1, wherein the second component is operative to cause at least one second identity data to be accessed, wherein the second component is operative to cause to be generated the at least one second authentication hash from the at least one second identity data and the at least one hashing argument.

3. The machine according to claim 2, further comprising a safe, wherein the transaction function device includes an input device, wherein the input device is located within the safe, wherein the computer is located outside the safe, wherein the second component is operative responsive to an input received through the input device to accept the at least one first identity data from the computer, wherein the accessed at least one second identity data corresponds to the accepted at least one first identity data.

4. The machine according to claim 3, wherein the transaction function device includes at least one data store, wherein the second component is operative to store the accepted at least one first identity data in the at least one data store of the transaction function device.

5. The machine according to claim 4, wherein the computer includes at least one hardware device, wherein the at least one hardware device includes the at least one first identity data stored therein.

6. The machine according to claim 4, wherein the at least one first identity data includes a serial number associated with the processor of the computer.

7. The machine according to claim 4, wherein the computer includes a hard drive, wherein the at least one first identity data includes a serial number associated with the hard drive.

8. The machine according to claim 1, wherein the second component is operative to cause to be determined at least three different levels of trust responsive to the comparison between the at least one first authentication hash and the at least one second authentication hash.

9. The machine according to claim 8, wherein the transaction function device is operative to perform a plurality of operations responsive to encrypted messages received from the first component, wherein the second component is operative to selectively enable and disable the operations responsive to the determined level of level.

10. The machine according to claim 1, wherein the at least one first identity data includes a plurality of first serial numbers, wherein the at least one first authentication hash includes a plurality of first authentication hashes, wherein the first component is operative to cause a plurality of different first authentication hashes to be generated from different combinations of the plurality of first serial numbers and the at least one hashing argument, wherein the at least one second authentication hash includes a plurality of second authentication hashes, wherein the second component is operative to cause the plurality of second authentication hashes to be compared to the plurality of first authentication hashes.

11. The machine according to claim 10, wherein the second component is operative to determine at least three different levels of trust responsive to the number of first authentication hashes which correspond to the second authentication hashes.

12. The machine according to claim 11, wherein the transaction function device is operative to perform a plurality of operations, wherein the second component is operative to cause the transaction function device to perform: none of the operations, a subset of the operations, or all of the operations responsive to the determined level of level.

13. The machine according to claim 11, wherein the second component is operative to case to be sent at least one message to the first component which includes data representative of the determined level of trust.

14. The machine according to claim 13, wherein the first component is operative to determine which types of messages to send to the second component responsive to the determined level of trust.

15. The machine according to claim 11, wherein the transaction function device includes a cash dispenser, wherein when all of the plurality of first authentication hashes corresponds to the plurality of second authentication hashes, the second component is operative to enable the cash dispenser to dispense cash in response to an encrypted messages received from the first component that is representative of a command to dispense cash.

16. The machine according to claim 15, wherein when none of the plurality of first authentication hashes corresponds to the plurality of second authentication, the second component is operative to prevent the cash dispenser from dispensing cash in response to an encrypted messages received from the first component that is representative of a command to dispense cash.

17. The machine according to claim 11, wherein the transaction function device is capable of performing a plurality of different operations responsive to encrypted messages received from the first component, wherein when at least one of the plurality of first authentication hashes is equal to a corresponding at least one of the plurality of second authentication hashes, and at least one of the plurality of first authentication hashes does not equal to a corresponding at least one of the plurality of second authentication hashes, the second component is operative to

permit the transaction function device to perform at least one of the operations responsive to a first type of encrypted message received from the first component, and the second component is operative to prevent the transaction function device from performing at least one of the operations responsive to a second type of encrypted message received from the first component.

18. The machine according to claim 11, wherein the transaction function device includes at least one data store, wherein the second component is operative to cause a plurality of second serial numbers to be accessed from the at least one data store, wherein the second component is operative to cause the plurality of second authentication hashes to be generated from different combinations of the plurality of second serial numbers retrieved from the data store and the at least one hashing argument.

19. The machine according to claim 1, wherein the first component is operative to cause the at least one encrypted message to be encrypted with the secret key and the second component is operative to cause the at least one encrypted message to be decrypted with the secret key.

20. The machine according to claim 1, wherein each of the first and second components is operative to independently cause a further secret key to be generated from the secret key, wherein the first component is operative to cause the at least one encrypted message to be encrypted with the further secret key and the second component is operative to cause the at least one encrypted message to be decrypted with the further secret key.

21. The machine according to claim 1, wherein the hashing argument includes the primary key.

22. The machine according to claim 21, wherein the second component is operative to cause the primary key to be sent to the first component.

23. The machine according to claim 1, wherein the second component is operative to provide a SessionID, wherein the second component is operative to cause a message to be sent to the first component which includes the SessionID and the public key of the second component.

24. The machine according to claim 23, wherein the first component is operative to cause the message sent from the first component to the second component which includes the encrypted secret key and the at least one first authentication hash, to further include the SessionID, wherein the second component is operative to determined that the Session ID received from the first component corresponds to the SessionID provided by the second component prior to enabling the transaction function device to perform a transaction function in response to the at least one encrypted message received from the first component.

25. The machine according to claim 1, wherein the first component is operative to encrypt the at least one first authentication hash using the secret key, wherein the at least one message includes the encrypted at least one first authentication hash, wherein the second component is operative to decrypt the encrypted at least one first authentication hash using the secret key decrypted with the public key.

26. The machine according to claim 1, wherein the transaction function device includes a cash dispenser, wherein the second component is operative to enable the transaction function device to dispense cash in response to the at least one encrypted message received from the first component.

27. The machine according to claim 1, wherein the transaction function device includes a cash recycler.

28. An automated banking machine comprising:

a computer, wherein the computer includes at least one hardware device, wherein the hardware device includes at least one serial number;

a cash dispenser in operative connection with the computer, wherein the cash dispenser includes an input device;

a safe, wherein the input device of the cash dispenser is located within the safe, wherein the computer is located outside the safe, wherein the cash dispenser is responsive to an input received from the input device to cause the cash dispenser to accept the at least one serial number of the hardware device, wherein the cash dispenser is operative to establish a secure communication session with the computer responsive to the accepted

serial number, wherein the cash dispenser is operative to dispense cash responsive to at least one message received through the secure communication session.

29. The machine according to claim 28, wherein the cash dispenser includes at least one data store, wherein the cash dispenser is operative to store the received serial number in the at least one data store of the cash dispenser.

30. The machine according to claim 28, wherein the cash dispenser includes a processor, wherein the processor is operative to generate at least one authentication hash from the serial number and at least one hashing argument, wherein the cash dispenser is operative to establish a secure communication session with the computer responsive to the at least one authentication hash.

31. The machine according to claim 28, wherein the hashing argument is a public key associated with the cash dispenser.

32. A method comprising:

a) accessing at least one first identity data with a computer in an automated banking machine from at least one hardware device of the computer;

b) generating with the computer at least one first authentication hash from the at least one first identity data and at least one hashing argument;

c) generating with the computer a randomly generated secret key;

d) encrypting with the computer the secret key using a public key associated with a transaction function device of the automated banking machine;

e) sending at least one message from the computer to the transaction function device which includes the encrypted secret key and the at least one first authentication hash;

f) decrypting the secret key with the transaction function device using a private key that corresponds to the public key of the transaction function device;

g) comparing with the transaction function device, the at least one first authentication hash to at least one second authentication hash; and

h) responsive to step (g) enabling the transaction function device to perform at least one transaction function in response to at least one encrypted message received from the first component.

33. The method according to claim 32, wherein prior to step (j) further comprising:

i) accessing at least one second identity data with the transaction function device; and

j) generating with the transaction function device, the at least one second authentication hash from the at least one second identity data and the at least one hashing argument.

34. The method according to claim 33, wherein the automated banking machine includes a safe, wherein the transaction function device includes an input device, wherein the input device is located within the safe, wherein the computer is located outside the safe, further comprising:

k) receiving an input from the input device;

l) responsive to step (k), accepting with the transaction function device, the at least one first identity data from the computer, wherein in step (i) the accessed at least one second identity data corresponds to the accepted at least one first identity data.

35. The method according to claim 34, further comprising:

m) storing the accepted at least one first identity data in at least one data store of the transaction function device.

36. The method according to claim 35, wherein in step (a) the at least one first identity data corresponds to a serial number of the at least one hardware device.

37. The method according to claim 35, wherein in step (a) the at least one first identity data includes a serial number associated with a processor of the computer.

38. The method according to claim 35, wherein in step (a) the computer includes a hard drive, wherein the at least one first identity data includes a serial number associated with the hard drive.

39. The method according to claim 32, wherein prior to step (h) further comprising:

i) determining a level of trust from among at least three different levels of trust responsive to step (g).

40. The method according to claim 39, wherein step (h) is performed responsive to the determined level of trust.

41. The method according to claim 32, wherein the at least one first identity data includes a plurality of first serial numbers, wherein the at least one first authentication hash includes a

plurality of first authentication hashes, wherein step (b) includes generating a plurality of different first authentication hashes from different combinations of the plurality of first serial numbers and the at least one hashing argument, wherein the at least one second authentication hash includes a plurality of second authentication hashes, wherein step (g) includes comparing the plurality of second authentication hashes to the plurality of first authentication hashes.

42. The method according to claim 41, wherein prior to step (h) further comprising:

i) determining a level of trust from among at least three different levels of trust responsive to the number of first authentication hashes which correspond to the second authentication hashes.

43. The method according to claim 42, wherein in step (i) the at least three different levels of trust include: fully trusted, partially trusted, and not trusted.

44. The method according to claim 42, wherein prior to step (h) further comprising

j) sending from the transaction function device to the computer, at least one message which includes data representative of the determined level of trust.

45. The method according to claim 44, after step (j) further comprising:

k) determining with the computer, which types of messages may be sent to the transaction function devices responsive to the determined level of trust.

46. The method according to claim 42, wherein the transaction function device includes a cash dispenser, wherein in step (g) when all of the plurality of first authentication hashes corresponds to the plurality of second authentication hashes, in step (h) the cash dispenser is enabled to dispense cash in response to an encrypted messages received from the computer that is representative of a command to dispense cash.

47. The method according to claim 46, wherein in step (g) when none of the plurality of first authentication hashes corresponds to the plurality of second authentication, in step (g) the cash dispenser is not operative to dispensing cash in response to an encrypted messages received from the computer that is representative of a command to dispense cash.

48. The method according to claim 42, wherein the transaction function device is capable of performing a plurality of different operations responsive to encrypted messages received from the computer, wherein in step (g) when at least one of the plurality of first authentication hashes is equal to a corresponding at least one of the plurality of second authentication hashes, and at least one of the plurality of first authentication hashes does not equal to a corresponding at least one of the plurality of second authentication hashes, in step (h) the transaction function device is enabled to perform at least one of the operations responsive to a first type of encrypted message received from the computer, and the second component is operative to prevent the transaction

function device from performing at least one of the operations responsive to a second type of encrypted message received from the computer.

49. The method according to claim 42, wherein the transaction function device includes at least one data store, further comprising:

j) accessing with the transaction function device, a plurality of second serial numbers from the at least one data store;

k) generating with the transaction function device, the plurality of second authentication hashes from different combinations of the plurality of second serial numbers retrieved from the data store and the at least one hashing argument.

50. The method according to claim 32, wherein prior to step (h) further comprising:

i) encrypting with the computer, at least one message to produce the at least one encrypted message using the secret key; and

j) decrypting with the transaction function device the at least one encrypted message with the secret key.

51. The method according to claim 32, further comprising:

i) independently generating by each of the computer and transaction function device, a further secret key from the secret key, wherein prior to step (h)

j) encrypting with the computer, at least one message to produce the at least one encrypted message using the further secret key; and

k) decrypting with the transaction function device the at least one encrypted message with the further secret key.

52. The method according to claim 32, wherein in step (b) the hashing argument includes the primary key associated with the transaction function device.

53. The method according to claim 52,wherein prior to step (d) further comprising:

i) sending the primary key from the transaction function device to the computer.

54. The method according to claim 32, wherein prior to step (d) further comprising:

i) providing a SessionID with the transaction function device;

j) sending a message from the transaction function device to the computer, wherein the message includes the SessionID and the public key associated with the transaction function device.

55. The method according to claim 54, wherein after step (e) the at least one message further include the SessionID, wherein prior to step (h) further comprising:

k) determining with the transaction function device that the Session ID sent in the at least one message in step (e) corresponds to the SessionID provided by the transaction function device in step (i).

56. The method according to claim 32, wherein prior to step (e) further comprising:

i) encrypting with the computer, the at least one first authentication hash using the secret key, wherein in step (e) the at least one message includes the encrypted at least one first authentication hash;

wherein prior to step (g) further comprising:

j) decrypt with the transaction function device, the encrypted at least one first authentication hash using the secret key decrypted in step (f).

57. The method according to claim 32, wherein in step (d) the transaction function device includes a cash dispenser, wherein in step (h) the transaction function device is enabled to dispense cash in response to the at least one encrypted message received from the computer.

58. The method according to claim 32, wherein in step (d) the transaction function device includes a cash recycler.

59. Computer readable media bearing instructions which are operative to cause the computer in the machine to cause the machine to carry out the method steps recited in claim 32.

60. A method comprising:

a) receiving with an input device at least one input, wherein the input device is associated with a cash dispenser of an automated banking machine, wherein the input device is located within a safe of the automated banking machine;

b) responsive to step (a), accepting with the cash dispenser at least one serial number of a hardware device of a computer of the automated banking machine, wherein the computer is located outside the safe;

c) establishing a secure communication session between the computer and the cash dispenser responsive to the accepted serial number; and

d) dispensing cash with the cash dispenser responsive to at least one message received through the secure communication session.

61. The method according to claim 60, wherein the cash dispenser includes at least one data store, wherein after step (b) further comprising:

e) storing the at least one serial number in the at least one data store of the cash dispenser.

62. The method according to claim 60, wherein after step (b) further comprising:

e) generating with the cash dispenser, at least one authentication hash from the serial number and at least one hashing argument, wherein in step (e) the cash dispenser is operative to enable the secure communication session to be established with the computer responsive to the at least one authentication hash.

63. The method according to claim 60, wherein in step (e) the hashing argument is a public key associated with the cash dispenser.

64. Computer readable media bearing instructions which are operative to cause the computer in the machine to cause the machine to carry out the method steps recited in claim 60.